



Charles Lehmann <charles@soundgateway.com> on 02/01/2002 03:58:30 PM

To: vss@FEC
cc: Anthony Boldin <anthony@atomicpark.com>
Subject: Comments on Voting Standards

To whom it may concern:

Attached are our comments on the revised voting standards. Please take the time to review our requested changes.

Thanks,
Charles Lehmann &
Anthony Boldin
RAM Software Development



. comments_on revised VSS Standards.rtf

To whom it may concern:

To help you more easily understand our comments and suggestions for change we have identified the specific section that we are citing in black, and then given both a requested change and reasoning for that requested change in blue.

Thanks for taking the time to review our comments!

Sincerely,
Charles Lehmann &
Anthony Boldin

Charles L. Lehmann &
Anthony T. Boldin
Ram Software Development
757 N. Broadway Suite #400
Milwaukee, WI 53202

Volume I

1.5.3

"It produces a tabulation of the voting data stored in a removable memory component and as printed copy."

Requested Change:

"It produces a tabulation of the voting data stored some form of removable, unalterable, electronic media" and "has the ability to be printed" instead of "a printed copy"

Reasoning:

The section should be changed to some form of removable, unalterable, electronic media to more fully encompass all possible removable storage solutions. Additionally, the election officials should have a choice as to when they want to print out the actual paper copy of the election results. In some situations printing out paper results immediately could be a liability.

1.6.1 Qualification Tests

Requested change and reasoning combined:

With today's technology and the advanced capabilities of today's testing laboratories it would be highly advantageous to let one laboratory perform both the hardware and software testing. For example, companies using off the shelf hardware would not have a clearly defined need for a hardware-testing agency. Rather it might be better to let the software agency perform all of the certification. Regardless, if this thought is not implemented the actual role of the testing agencies and how they should work together should be more clearly defined in this document. Otherwise, the testing agencies themselves rather than the law will continue to define this role.

2.2.5.2.1 letter g. "The printer shall print a copy of the audit record."

Requested Change: "The printer shall be capable of printing a copy of the audit record." Also, it should be defined in this section what exactly printing an audit record is: every auditable piece of data, images of the ballot, all data base information etc.

Reasoning:

Due to the possible length of audit records this section should be reworded so that it defines more specifically what needs to be printed. If a DRE system were to monitor all of the events and its system status on a regular basis audit records could possibly be extremely lengthy. It would be extremely advantageous for the auditor to be able to specify only the exact portion of the audit records that they need.

2.2.7.2 letter b, c, d. System is required to have audio functionality.

Requested Change: "Systems should be capable of being equipped with audio functionality or some process to aid visually impaired voters."

Reasoning:

I agree that it is necessary to make provisions for handicapped individuals; however, having the requirement of audio functionality on every machine is extreme and may cause a needless rise in the price of voting equipment. Additional section 6.5 of Volume to states that Voting machines intended for use by voters with disabilities provide the capabilities required by Volume I, Section 2.2.7 indicating that not every voting system needs to provide audio capabilities to handicapped users.

1.1.1.2 Letter e.

Requested Change:

"Adjusting screen contrast should be a required function that can be instituted by an election official."

Reasoning:

While it may seem like a nice option for voters to be able to adjust the contrast of the screen themselves, it is more appropriate that this functionality would be performed by an election official. Specifically, in touch screen devices, controls that allowed the user to adjust the contrast and screen size could cause users to put their touch screens into a state that is out of calibration. A touch screen that was out of calibration would make the touch screen very difficult to use and inaccurate with respect to the users prompts. Additionally, allowing every voter to play with the contrast of their screens would slow down voting considerably.

2.2.9.2 Letter d.

Requested Change:

"The lifecycle counter should be visible to election officials."

Reasoning:

Displaying the lifecycle counter to the voter is really not a wise use of screen real estate.

2.3.1.3.1 Common Standards

a. The electronic display or printed document on which the user views the ballot is capable of rendering an image of the ballot in any of the languages required by The Voting Rights Act of 1965, as amended;

Requested Change:

"The electronic display or printed document on which the user views the ballot is capable of rendering an image of the ballot in any of the standard keyboard languages."

Reasoning:

Requiring the incorporation of to many languages beyond such common foreign languages as Spanish, German, etc., such as Japanese that uses symbols would greatly increase the cost of electronic voting systems to users.

2.4.3.1 Common Standards

f. Provide the capability for the voter to cast a ballot in the event of a failure of power supply external to the voting system

Requested Change:

"Allow for the graceful shutdown of the voting system and allow from the any voters to resume their vote once back-up power has been reverted to."

Reasoning:

This would ensure that voters never lost their votes, while providing provisions for failure that aren't extremely expensive.

3.2.2.4 Electrical Supply

c. All systems shall also be capable of operating for a period of at least 16 hours on backup power. This capability shall include the provision of all power required to:

- 1) Activate voting, record votes, and count ballots (in DRE systems);
- 2) Count ballots (in paper-based systems);
- 3) Display all system status and error messages; and
- 4) Maintain the contents of program and data memory.

"The voting location should provide backup power that lasts for at least 16 hours such as a backup generator."

Reasoning:

To continue voting power would need to be provided for multiple things in addition to the DRE's such as power to the lighting, doors, and phones, etc... A commercial backup power supply that would run a standard voting system for a 1 hour costs over \$100. Therefore, with existing technology 16 hours of backup power would cost \$1600 dollars for every DRE system. Such a figure is to high a number to allow 16 hours of backup power to be cost effectively incorporated into DRE systems. Therefore, one is left with no resort, but to call for the actual voting location to provide that entire 16 hours of backup power with something such as a generator.

3.2.4.3.2 DRE System Vote Recording

c. Provide at least two processes that record the voter's selections that:

- 1) Use neither common software nor common storage devices for these processes;

What is the reasoning behind this? This sounds like it could eliminate such storage components as our CDR and a typical hard drive. It would be interesting to find out what they consider common storage devices?

No kidding - why wouldn't you want to use common storage devices. Our argument is that the common storage devices are those that are the most reliable - why would you even need to create anything - and not only that any device could be contrived as common - this one is really dumb.

3.2.6.2.1 Processing Speed

b. Extract voting data from a voting device by electronic means in a time not to exceed one minute; and

Requested Change:

"Extracting voting data from a voting device should not take an exorbitant amount of time."
Or remove part from the standards.

Reasoning:

If one were to extract all of the data from the voting machine including audit data significant amounts of data may have to be extracted (500MB). One minute is extremely fast to transfer this amount of data. If this requirement is really necessary, exactly what needs to be extracted in 1 minute from the voting device needs to be more clearly defined.

3.3.3 Transport and Storage of Precinct Systems

a. Provide a handle or handles to facilitate their handling, transport, and installation;

Requested Change:

A handle for transportation should not be required.

Reasoning:

The standards should merely read that there should be means to safely and easily transport and install equipment. For example what if the method of transportation of some system was wheels rather than a handle.

6.4 Software and Firmware Installation

b. To prevent alteration of executable code, no software shall be permanently installed or resident in the system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware.

Requested Change:

"To prevent alteration of the executable code, no software shall permanently installed or resident in the system unless there is some method that proves that the software has not be changed since its installation or the system documentation...."

Reasoning:

If there is some way to verify that the software code that is resident to the machine has not been changed since installation it logically follows that it should not be a requirement for the jurisdiction to store the system in a secure place.

VOLUME II

6.2.2 System for Baseline Testing

The system level qualification tests are conducted using the version of the system as it is intended to be sold by the vendor and delivered to jurisdictions. To ensure that the system version tested is the correct version, the ITA shall witness the build of the executable version of the system immediately prior to or as part of the physical configuration audit. Additionally, should components of the system be modified or replaced during the qualification testing process, the ITA shall require the vendor conduct a new "build" of the system to ensure that the qualified executable release of the system is built from tested components.

Requested Change:

This should not be a requirement.

Reasoning:

Even if the testing agency witnesses the build in person it does not ensure that someone couldn't slip in some unauthorized piece of code or component after hours. Therefore, having the testing agency witness the build does not really serve and purpose other than to increase the cost of certification for vendors.

One other note:

The standards call for significantly greater involvement of the testing agencies to ensure proper QA and configuration management. Included in this is the requirement that is mentioned multiple times throughout the standards that the ITA representative has to actually come to the vendors site to witness the system build. Refer to volume II section 7.2 "Basis of examinations"

Requested Change:

It shouldn't be mandatory for the testing agency to witness the system build. Rather the testing agency should verify through some type of process that the system as built contains the exact software and hardware that is being approved.

Reasoning.

Once again, having the ITA's actually witness the system build would accomplish not specific purpose other than to raise that cost of certification. Plus, I would like to refer to the possibility that even if an ITA did witness the system build it would still be possible for some mischievous soul to slip some altered component a software component into the system.

Thanks for taking the time to read and consider all of our comments and suggestions.

Sincerely,

Charles Lehmann &

Anthony Boldin

RAM Software Development